AMENDMENTS TO THE SPECIFICATION

Regarding Omission #1, please replace the paragraph from page 2 ll. 19-20 with the following paragraph:

Document 2:

International Workshop LNCS.1636

Regarding Omission #2, please replace the paragraph from page 3 line 20 to page 4 line 2 with the following paragraph:

That is, the present invention provides a cipher strength estimating device for estimating a strength of a ciphertext which is a transformed text obtained at a final round of a transformation process including: receiving a plaintext; transforming the plaintext using, as a parameter, a session key calculated from a key for use in encryption; and repeatedly further transforming the resulting transformed text which is the plaintext thus transformed to perform stepwise encryption,

Regarding Omission #3, please replace the paragraph from page 5 line 23 to page 6 line 9 with the following paragraph:

This cipher strength estimating device, which is configured to calculate plural prospects in advance and reduce the number of such prospects in the process of calculating a key for the immediately preceding round, is more effective in reducing the amount of calculation and the like than the approach to find keys for respective rounds separately. Further, the feature that a session key for the immediately preceding round is found on the assumption that a certain session key prospect is the session key, is capable of finding out plural session keys at an earlier

stage than by the approach to complete calculations of all session key prospects for each round before calculating the session key prospect for the immediately preceding round.

Regarding Omission #4, please replace the paragraph from page 7 line 23 to page 8 line 14 with the following paragraph:

the control unit is operative to: input the plaintext and one of the ciphertext obtained at the final round of the transformation process and the putative transformed text obtained at the certain intermediate round, which make a pair, to the untransformed text calculating unit; receive the putative untransformed text outputted; repeatedly further input the putative untransformed text as a putative transformed text for a round immediately preceding the relevant round to the untransformed text calculating unit together with the plaintext; and optionally output the recalculation request data to the session key prospect calculating section in response to receipt of the uncalculability identifier data outputted from the session key prospect calculating section to cause the session key prospect calculating section to again calculate said another session key prospect for the immediately preceding round and then output the putative untransformed text based on said another session key prospect.

Regarding Omission #5, please replace the paragraph on page 10 lines 4-11 with the following paragraph:

the untransformed text calculating unit body is operative to calculate the putative untransformed text presumed to be equivalent to an untransformed text which is not transformed yet at the relevant round based on the session key prospect and one of the ciphertext and the putative transformed text; and output the putative untransformed text as an output of the untransformed text calculating unit; and

Regarding Omission #6, please replace the paragraph on page 12 lines 11-16 with the following paragraph:

the second untransformed text calculating unit is operative to receive, as inputs thereto, the plaintext and one of the ciphertext obtained at the final round of the transformation process and a putative transformed text presumed to be a transformed text obtained at a certain intermediate round;

Regarding Omission #7, please replace the paragraph on page 14 lines 13-23 with the following paragraph:

This configuration uses two types of session key calculating units to dynamically create the conditions based on an algebraic method utilizing higher order differential cryptanalysis at a certain round and then judges a session key prospect for this round to be false based on the conditions without actually calculating the session key. Thus, even in finding out session keys for two or more rounds, the total amount of calculation can be reduced though the brute-force search imposing a high load is employed at the immediately succeeding round, as long as the cipher has a transforming block like MISTY1 for example.

Regarding Omission #8, please replace the paragraph from page 15 line 24 to page 16 line 6 with the following paragraph:

Fig. 2 is a block diagram illustrating the system configuration of a cipher strength estimating device according to this embodiment. The cipher strength estimating device is, for example, a general-purpose computer as shown and includes a CPU 101, internal memory 102, an external storage unit 103 such as HDD, a communication interface 104, such as a modem, for

providing connection to a communication network, a display 105, input means 106 such as a mouse or a keyboard, and the like, as shown in Fig. 3.

Regarding Omission #9, please replace the paragraph on page 17 lines 16-21 with the following paragraph:

As a result of investigation on effective plaintexts, which make a slow increase in degree, a plaintext obtained by varying only the rightmost sub-block with the rest fixed was found effective. Accordingly, the plaintext and ciphertext calculating unit 3 is configured to calculate a pair of plaintext and ciphertext satisfying such a condition.

Regarding Omission #10, please replace the paragraph on page 19 lines 16-19 with the following paragraph:

The plaintext outputted from the plaintext and ciphertext calculating unit contains a 7-bit variable. For a cryptanalysis using 7^{th} order differential to be employed, first, a sub-space $V^{(7)}$ is determined as

Regarding Omission #11, please replace the paragraph on page 22 lines 8-23 with the following paragraph:

The control unit inputs the plaintext and the ciphertext obtained at the final round of the transformation process, which make a pair, to the first untransformed text calculating unit, receives a 6^{th} round putative untransformed text outputted and further inputs the putative untransformed text as a putative untransformed text for the 5^{th} round to the second untransformed text calculating unit together with the plaintext. Alternatively, in response to receipt of the uncalculability identifier data outputted from the second session key prospect calculating section, the control unit outputs the recalculation request data to the first session key

prospect calculating section to cause the first session key prospect calculating section to calculate another 6th round session key prospect and outputs a putative untransformed text for the 5th round based on said another session key prospect.

Regarding Omission #12, please replace the paragraph on page 24 lines 9-18 with the following paragraph:

The second untransformed text calculating unit 22 receives the plaintext and the 5th round putative transformed text, and the second session key prospect calculating section 22K included in the second untransformed text calculating unit 22 creates conditions for calculation of a 5th round session key prospect dynamically by the use of the 5th round putative transformed text and then performs calculation by an algebraic method or outputs the uncalculability identifier data if the conditions thus created include conditions that are inconsistent with each other.

Regarding Omission #13, please replace the paragraph on page 26 lines 13-23 with the following paragraph:

If a putative untransformed text outputted from a certain putative untransformed text calculating unit of the cipher strength estimating device of the present invention is used as an input to a different cipher strength estimating device, or if a putative untransformed text outputted from a different cipher strength estimating device is used as an input to a certain putative untransformed text calculating unit of the cipher strength estimating device of the present invention, the present invention becomes applicable to the estimation of a cipher from a different cipher strength estimating device.

Regarding the omitted drawing Figure 8, please delete the paragraph on page 15 ll. 18-19 and replace the paragraph on page 21 ll. 5-7 with the following paragraph:

The key K can be moved by transforming the key in the modified MISTY1 ~~as shown in Fig. 8~~. Since KL is divided into K_{Ll} and K_{Lr} ($\in$GF(2)16) in FO5 function, the following holds in FI_{51}.